IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

DOMINIC FIACCO, individually and on behalf of all others similarly situated, Plaintiff, v. UNIVERSITY OF ROCHESTER, Defendant.	Civil Action No. 6:23-cv-972 (DNH/TWD) **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Dominic Fiacco ("Plaintiff") brings this action on behalf of himself and all others similarly situated against Defendant University of Rochester ("Rochester" or "Defendant"). Plaintiff makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to the allegations specifically pertaining to himself, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiff brings this action against Defendant as a result of Defendant's failure to safeguard and protect the confidential information of Plaintiff and the other members of the Class — including Social Security Numbers and personal information that can be used to perpetrate identity theft — in Defendant's custody, control, and care (the "Sensitive Information").

2. Plaintiff is an incoming student at the University of Rochester. As a condition of Plaintiff's attendance, Plaintiff was required to and did supply Sensitive Information to Defendant, including, but not limited, to his Social Security Number, date of birth, financial information, and other personal private data.

3. Unbeknownst to Plaintiff, Defendant did not have sufficient cyber-security

procedures and policies in place to safeguard the Sensitive Information it possessed. Indeed, Defendant disclosed Plaintiff's and Class Members' Sensitive Information to a third-party, Progress Software, which had a security vulnerability in its MOVEit File Transfer solution, a system which was used by Defendant. As a result, cybercriminals were able to gain access to University of Rochester data, including Plaintiff and Class Members' Sensitive Information, on May 27, 2023, thereby gaining access to approximately 88,000 Class Members' Sensitive Information, including Plaintiff's (the "Data Breach"). Plaintiff and members of the proposed Class have suffered damages as a result of the unauthorized and preventable disclosure of their Sensitive Information. Indeed, following the Data Breach, Plaintiff experienced a fraud issue with his bank account.

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity protections and protocols that were necessary to protect the Sensitive Information of students entrusted into Defendant's custody and care.

5. This lawsuit seeks to redress Defendant's unlawful disclosure of the Sensitive Information of all persons affected by this Data Breach.

PARTIES

6. Plaintiff Dominic Fiacco is and was a resident of Newport, New York, who was an incoming freshman at the University of Rochester when the Data Breach occurred, and whose Sensitive Information was compromised in the Data Breach.

7. The Data Breach occurred on May 27, 2023.

8. Defendant was notified of the Data Breach on May 31, 2023.

9. On June 13, 2023 — after Defendant had already been notified of the Data Breach but had not yet informed Plaintiff of the Data Breach — Plaintiff was notified of a fraud issue

with his bank account. Specifically, a criminal took thousands of dollars out of Plaintiff's bank account, without Plaintiff's knowledge or consent.

10. As a result, Plaintiff had to spend time working with his bank to investigate the fraudulent activity, and to receive provisional credit from his bank for the several thousand dollars that were taken from his account.

11. Defendant did not send out a notification email to Plaintiff regarding the Data Breach until July 25, 2023. That email referenced an "update to [a] June 2 message about a cybersecurity incident at the University of Rochester," but Plaintiff never received any message on June 2, 2023.

12. Defendant did not send out a physical notification letter to Plaintiff regarding the data breach until July 28, 2023.

13. Plaintiff did not receive the physical notification letter from Defendant regarding the data breach until August 7, 2023. A copy of that letter is attached hereto as Exhibit A.

14. The physical notification letter from Defendant stated that Plaintiff's Sensitive Information, including his Social Security Number, may have been compromised as a result of the Data Breach.

15. Plaintiff had never experienced identity, credit, or financial fraud or theft prior to the Data Breach.

16. Plaintiff had never had any of his personal information or Sensitive Information exposed in a data breach prior to the May 27, 2023 Data Breach.

17. Defendant University of Rochester is a private university located in Rochester, New York.

JURISDICTION AND VENUE

18. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendant because the wrongful conduct giving rise to this case occurred in, was directed to, and/or emanated from this District, and because a substantial portion of the events giving rise to Plaintiff's claims occurred in this District, including Plaintiff's provision of his Sensitive Information to Defendant.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to this claim occurred in this District.

FACTUAL ALLEGATIONS

The Risks of Data Breaches and Compromised Sensitive Information are Well Known

21. Defendant University of Rochester had obligations created by contract, industry standards, common law, and representations made to current, former, and prospective students to keep Plaintiff's and Class Members' Sensitive Information confidential and to protect it from unauthorized access and disclosure.

22. Defendant's data security obligations are and were particularly important given the substantial increase in cyberattacks and/or data breaches widely reported on in the last few years. In fact, in the wake of this rise in data breaches, the Federal Trade Commission has issued an abundance of guidance for companies and institutions that maintain individuals' Sensitive

Information.[1]

23. Therefore, Defendant knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place.

Defendant Allowed Criminals to Obtain Plaintiff's and the Class' Sensitive Information

24. Plaintiff and Class Members were obligated to provide Defendant with their Sensitive Information as part of their relationships with Defendant.

25. Due to inadequate security against unauthorized intrusion, including but not limited to Defendant's disclosure of Plaintiff and Class Members' Sensitive Information to a third-party, cybercriminals breached Plaintiff's and the Class' Sensitive Information on or about May 27, 2023. This Data Breach resulted in the criminals unlawfully obtaining access to students' Sensitive Information, including their identities and Social Security Numbers.

Data Breaches Lead to Identity Theft

26. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victims' name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.

27. Indeed, Plaintiff has already been the victim of bank fraud following the Data Breach, which resulted in thousands of dollars being stolen from his bank account and cost him time in addressing the fraud.

28. As the United States Government Accountability Office noted in a June 2007

[1] *See, e.g.*, *Protecting Personal Information: A Guide for Business,* FTC, *available at* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Aug. 9, 2023).

report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[2] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

29. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconvenience repairing damage to their credit records."[3]

30. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phones or utilities fraud, and bank/finance fraud.

31. There may be a time lag between when sensitive information is stolen and when it is used. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[4]

32. With access to an individual's Sensitive Information, cyber criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's

---

[2] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/products/gao-07-737 (last visited Aug. 9, 2023).

[3] *Id.* at 9.

[4] *Id.* at 29

picture; using the victim's name and Social Security Number to obtain government benefits; or filing a fraudulent tax return using the victim's information.

33. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security Numbers, and other Sensitive Information directly on various Internet websites making the information publicly available.

34. On or about July 28, 2023, Defendant sent letters to Plaintiff and other Class members advising them that their Sensitive Information had been subject to unauthorized access and had been compromised on or about May 27, 2023 (the "Letter Notification"). A copy of the Letter Notification that Plaintiff received is attached as **Exhibit A** to this Complaint. The Letter Notification offered only two years of credit monitoring through Experian IdentityWorks, however, and only for individuals who sign up for such monitoring by October 7, 2023.

Defendant's Obligations and Its Negligent Failure to Meet Them

35. In the ordinary course of, and as a condition of, his enrollment as a student at University of Rochester, Plaintiff, like thousands of other students, alumni, applicants, faculty, and/or staff, provided Sensitive Information, including but not limited to his Social Security Number, to Defendant.

36. Defendant University of Rochester maintains this Sensitive Information within its data infrastructure, including within third-party vendors' systems as a result of Defendant's disclosures to said third-parties such as Progress Software.

37. Furthermore, Plaintiff and Class Members all entered into agreements with

Defendant as part of, and as a precondition to, application and enrollment at the University of Rochester. These agreements contained or implied representations that Defendant would protect Members' Sensitive Information.

38. Indeed, Defendant publicly posts policies regarding information security, including an "Information Technology Policy."[5]

39. Defendant's Policy states that it "applies to everyone who accesses University Information Technology Resources, whether affiliated with the University or not, whether on campus or from remote locations, including but not limited to students, faculty, staff, contractors, consultants, temporary employees, guests, and volunteers."[6]

40. The Policy notes that "there are types of information where access must be restricted and caution in handling and storing the information is necessary." [7]

41. The PDF version of the Policy bears an "adopted" date "December 12, 2006" and a "last revised" date of "January 17, 2019" indicating it was in effect at all relevant times herein.[8]

42. The Policy specifies several categories of information as "High Risk Information," including "Social Security Numbers (SSN)[,] Patient Protected Health Information (HIPAA)[,] Student Information (FERPA)[,] Financial Account, Credit and Debit Card Information[,] and Employee Personnel Records."[9] Defendant requires that "High Risk Information in electronic form must be stored in secure designated data centers or, if authorized

[5] https://tech.rochester.edu/policies/information-technology-policy/ (last visited Aug. 9, 2023) (Defendant's "Policy").

[6] *Id.*

[7] *Id.*

[8] https://tech.rochester.edu/wp-content/uploads/2015/09/Information-Technology-Policy-Jan-2019.pdf (last visited Aug. 9, 2023)

[9] https://tech.rochester.edu/policies/information-technology-policy/ (last visited Aug. 9, 2023).

to be stored elsewhere, only in encrypted (or similarly protected) form," that "[i]t must not be stored on desktop, laptop or other portable devices or media without encryption or similar protection, and that "when a record containing High Risk Information is no longer needed, it must be disposed of in a manner that makes the High Risk Data no longer readable or recoverable." [10] The Policy additionally notes that "prompt reporting of unauthorized disclosure of High Risk Information is essential for the University to meets its obligations under law, regulation, and contract." [11]

43. The Policy also assigns further, specific policies to the protection of High Risk Information. The purpose of these additional policies is to provide a higher degree of care and protection when collecting and recording High Risk Information. For example, Defendant's "Social Security Number/Personally Identifiable Information Policy" notes that the "reasons for this Policy are to prevent identity theft through unauthorized use of an individual's SSN and/or PII and to comply with New York law," and states that the "University of Rochester will collect and record Social Security Numbers (SSN) and Personal Identifying Information (PII) only as necessary to comply with requirements of law, to support patient safety or to carry on necessary University functions."[12] Further, it provides that "[w]here a unique identification number is required for a purpose not based in law, contract or patient safety, the University will use a number other than SSN or, if there is no current reasonably feasible alternative, will maintain SSN in a secure environment" and that the "University will protect the confidentiality of the SSN that it holds and permit access to them only for legitimate University purposes."[13] The same

[10] *Id.*

[11] *Id.*

[12] https://tech.rochester.edu/policies/ssn-pii-policy/ (last visited Aug. 9, 2023)

[13] *Id.*

policy also notes that "[p]rompt reporting of unauthorized disclosure of Social Security Number and Personal Identifying Information is essential for the University to meets its obligations under law, regulation, and contract." [14]

44. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Sensitive Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Sensitive Information from unauthorized disclosure.

45. Defendant compounded the actual and potential harm arising from the Data Breach by not fully notifying Plaintiff and other Class Members of the extent of the compromise of their personal information until July 28, 2023, when the Letter Notification was sent. Defendant's delay in notifying Plaintiff and the Class the full extent to which they were victims of the Data Breach will dilute any salutary effect that might come from these suggestions.

46. Defendant's security failure demonstrates that it failed to honor its duties and promises by not:

(a) Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

(b) Adequately protecting Plaintiff's and the Class Members' Sensitive Information;

(c) Abiding by its own stated policies and procedures with respect to Sensitive Information;

(d) Properly monitoring its own data security systems for existing intrusions; and

(e) Ensuring that agents, employees, and others with access to Sensitive Information employed reasonable security procedures.

[14] *Id.*

47. Plaintiff and all members of the Class have consequently suffered harm by virtue of the compromise and exposure of their Sensitive Information – including, but not limited to, (i) an imminent risk of future identity theft; (ii) lost time and money expended to mitigate the threat of identity theft; (iii) diminished value of personal information; and (iv) loss of privacy. Plaintiff and Class Members were also injured because they did not receive the full value of services for which they bargained; educational services plus adequate data security. Plaintiff and all members of the proposed Class are and will continue to be at imminent risk for tax fraud and identity theft and the attendant dangers thereof for the rest of their lives because their Sensitive Information, including Social Security Numbers, is in the hands of cyber-criminals.

Defendant's Inadequate Response to the Data Breach

48. Defendant's Letter Notification stated that it "took immediate action to mitigate and assess the scope of information potentially compromised, including engaging outside professionals to assist in the investigation and remediating the vulnerability." No details were provided, and thus it cannot be determined from the Letter Notification whether Defendant did any of the foregoing, or if it did, whether these enhancements are sufficient to prevent recurrences similar to the Data Breach.

49. The belated Letter Notification also included an offer from Defendant of two years of free credit monitoring and identity theft resolution services through a third-party provider, Experian. Defendant, however, offered an unreasonably short window of opportunity to claim these services, with victims of the Data Breach needing to claim these services by October 7, 2023, or be closed out. In addition, two years of credit monitoring services is insufficient, given that Plaintiff's and the Class Members' risk of identity theft will continue throughout their lives.

50. Conspicuously absent from the Letter Notification is any offer of compensation for out-of-pocket losses which the Class has and foreseeably will sustain – including, but not limited to, time spent to rectify any and all harms that resulted from the Data Breach. Plaintiff and members of the Class have suffered financial loss, including but not limited to lost opportunity costs for the time and effort necessary to remedy the harm they suffered. Thus, Defendant's offer in the Letter Notification fails to make Plaintiff and the other members of the Class whole.

CLASS ALLEGATIONS

51. Plaintiff seeks to represent a class defined as:

> All persons whose Sensitive Information, provided to Defendant as part of their application to, enrollment at, or employment by the University of Rochester, was exposed to unauthorized access by way of the data breach on or about May 27, 2023. (Hereinafter, the "Class").

52. Plaintiff reserves the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

53. Plaintiff is a member of the Class.

54. Excluded from the Class are: (i) Defendant; any entity in which Defendant has a controlling interest; the officers and directors of Defendant; and the legal representatives, heirs, successors, and assigns of Defendant; (ii) any judge assigned to hear this case (or any spouse or family member of any assigned judge); (iii) any juror selected to hear this case; and (iv) any and all legal representatives (and their employees) of the parties.

55. Plaintiff additionally seeks to represent a subclass defined as "All members of the Class who are residents of New York." (Hereinafter, the "New York Subclass").

56. This action seeks both injunctive relief and damages.

57. Plaintiff and the Class satisfy the requirements for class certification for the

following reasons:

58. **Numerosity of the Class.** According to contemporaneous reporting of the Data Breach, the Data Breach affected approximately 88,000 individuals.[15] Therefore, the members of the Class are so numerous that their individual joinder is impracticable. The precise number of persons in the Class and their identities and addresses may be ascertained or corroborated from Defendant's records. If deemed necessary by the Court, members of the Class may be notified of the pendency of this action.

59. **Existence and Predominance of Common Questions of Law and Fact.** There are question of law and fact common to the Class that predominate over any questions affecting only individual members, including:

(a) Whether Defendant's data security systems prior to the Data Breach met the requirements of relevant laws;

(b) Whether Defendant's data security systems prior to the Data Breach met industry standards;

(c) Whether Plaintiff's and other Class Members' Sensitive Information was compromised in the Data Breach; and

(d) Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

60. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's grievances, like the proposed Class Members' grievances,

[15] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/c684da85-ab09-41bb-9daa-66bf522623c5.shtml (last visited Aug. 9, 2023).

all arise out of the same business practices and course of conduct by Defendant.

61. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel that is highly experienced in complex class action litigation, and Plaintiff intends to vigorously prosecute this action on behalf of the Class. Furthermore, Plaintiff has no interests that are antagonistic to those of the Class.

62. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense of individual litigation of their claims against Defendant. It would, thus, be virtually impossible for the Class on an individual basis, to obtain effective redress for the wrongs committed against them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances.

63. In the alternative, the Class may also be certified because:

(a) The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for the Defendant;

(b) The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the

interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

64. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

65. Defendant owed a duty to Plaintiff and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiff's and Class Members' Sensitive Information within its control from being compromised, by being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate security measures over its networks and systems — including third parties it disclosed the Sensitive Information to — so as to prevent unauthorized access thereof.

66. Defendant owed a duty of care to the Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that it adequately protected the Sensitive Information of the individuals who entrusted it to Defendant.

67. Only Defendant was in a position to ensure that its and its vendors' systems were sufficient to protect against the harm to Plaintiff and the members of the Class from the Data Breach.

68. In addition, Defendant had a duty to use reasonable security measures under Section A of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair …

practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

69. Defendant's duty to use reasonable care in protecting the Sensitive Information arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential information, as well as its own stated policies.

70. Defendant breached its common law, statutory, and other duties – and thus, was negligent – by failing to use reasonable measures to protect students' Sensitive Information, and by failing to provide timely notice of the Data Breach, and/or by failing to abide by its own stated policies. The specific negligent acts and omissions committed by Defendant include, but are not limited, to the following:

(a) Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the Class members' Sensitive Information;

(b) Failing to adequately monitor the security of its networks and systems;

(c) Failing to abide by its own stated policies with respect to Plaintiff's and the Class Members' Sensitive Information;

(d) Allowing unauthorized access to Plaintiff's and the Class Members' Sensitive Information; and

(e) Failing to warn Plaintiff and other Class Members about the full extent of the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

71. Defendant owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

72. It was foreseeable that Defendant's failure to use reasonable measures to protect Sensitive Information and to provide timely notice of the full extent of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

73. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff and the members of the Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

74. Defendant knew or reasonably should have known of the inherent risks in collecting and storing the Sensitive Information of Plaintiff and members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate cyber-security systems and protocols in place to secure the Sensitive Information.

75. As a result of the foregoing, Defendant unlawfully breached its duty to use reasonable care to protect and secure the Sensitive Information of Plaintiff and the Class which Plaintiff and members of the Class were required to provide to Defendant as a condition of application to or enrollment at the University of Rochester.

76. Plaintiff and members of the Class reasonably relied on Defendant to safeguard their information, and while Defendant was in a position to protect against harm from a data breach, Defendant negligently and carelessly squandered that opportunity. As a proximate result, Plaintiff and members of the Class suffered and continue to suffer the consequences of the Data breach.

77. Defendant's negligence was the proximate cause of harm to Plaintiff and members of the Class.

78. Had Defendant not failed to implement and maintain adequate security measures to protect the Sensitive Information of its students, the Plaintiff's and Class Members' Sensitive Information would not have been exposed to unauthorized access and stolen, and they would not have suffered any harm.

79. However, as a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiff and members of the Class have been injury by, among other things; (1) the loss of opportunity to control how their Sensitive Information is used; (2) diminution of value and the use of their Sensitive Information; (3) compromise, publication and/or theft of the Plaintiff's and the Class Members' Sensitive Information; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial accounts; (5) lost opportunity costs associated with their efforts expended and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the breach including, but not limited to, efforts spent researching how to prevent, detect, and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or

increased cost of the use, the use of credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised Sensitive Information to open new financial accounts; (8) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected and/or imminent risk of the foregoing; (9) continued risks to their Sensitive Information, which remains in Defendant's possession and may be subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its possession; and (10) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the Sensitive Information compromised as a result of the Data Breach as a remainder of the Plaintiff's and Class Members' lives.

80. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

COUNT II
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

81. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

82. Plaintiff and members of the Class provided Sensitive Information to Defendant in connection with their obtaining educational services from Defendant and were required to provide their Sensitive Information as a condition of receiving services therefrom.

83. Defendant would not have enrolled Plaintiff, nor enrolled and/or employed any members of the Class, had Plaintiff and members of the Class not provided various forms of Sensitive Information to Defendant, including their Social Security Numbers and other privileged and confidential items of information.

84. Plaintiff and members of the Class had no alternative and did not have any bargaining power with regards to providing their Sensitive Information. Defendant required disclosure of Sensitive Information as a condition to providing its services and/or employment, which the Plaintiff and members of the Class did.

85. When Plaintiff and Class Members paid money and provided their Sensitive Information to Defendant in exchange for services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

86. Defendant solicited and invited prospective students, employees, faculty, and others to provide their Sensitive Information as part of its regular business practices. These individuals accepted Defendant's offers and provided their Sensitive Information to Defendant. In entering into such implied contracts, Plaintiff and the Class reasonably assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

87. Plaintiff and the Class would not have provided and entrusted their Sensitive Information to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

88. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

89. Defendant breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of the Data Breach.

90. As a direct and proximate result of Defendant's breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

91. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

COUNT III
Breach of Express Contract
(On Behalf of Plaintiff and the Class)

92. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

93. Plaintiff and Class Members entered into written agreements with Defendant as part of, and as a precondition to, application to, enrollment in, and/or employment by the University of Rochester. These agreements contained or incorporated the representations outlined *supra* ¶¶ 37-43 that Defendant would protect and responsibly handle Class Members' Sensitive Information. The agreements involved a mutual exchange of consideration whereby Defendant provided (or committed to considering to provide) educational services and/or compensation for Class Members in exchange for payment or work, respectively, from Class Members.

94. Defendant's failure to abide by its own stated policies and Defendant's failure to protect Class Members' Sensitive Information constitute a material breach of the terms of the agreement by Defendant, as reflected, *inter alia*, in its policies relating to Sensitive Information outlined *supra*.

95. As a direct and proximate result of Defendant's breach of contract with Plaintiff and Class Members, Plaintiff and Class Members have been irreparably harmed.

96. Plaintiff and the Class seek damages, injunctive relief, and other and further relief

as the Court may deem just and proper.

COUNT IV
Violation Of New York General Business Law § 349
(On Behalf of Plaintiff and the New York Subclass)

97. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

98. Defendant, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade, and commerce and the furnishing of services, in violation of N.Y. GBL § 349(a). This includes but is not limited to the following:

(a) Defendant failed to enact adequate privacy and security measures to protect the New York Subclass Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

(b) Defendant failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Defendant knowingly and deceptively misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

(d) Defendant knowingly and deceptively misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information; and

(e) Defendant failed to abide by its own stated policies pertaining to the privacy and

security of Sensitive Information.

99. As a direct and proximate result of Defendant's practices, Plaintiff and other New York Subclass Members suffered injury and/or damages, including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

100. The above unfair and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and other New York Subclass Members that they could not reasonably avoid, which outweighed any benefits to consumers or to competition.

101. Defendant knew or should have known that its data security practices were inadequate to safeguard Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, and willful.

102. Plaintiff, on behalf of himself and the putative New York Subclass, seeks relief under N.Y. GBL § 349(h) for the greater of actual damages (to be proven at trial) and statutory damages of $50 per violation, injunctive relief, and/or attorneys' fees and costs.

103. Plaintiff and New York Subclass Members seek to enjoin the unlawful deceptive acts and practices described above. Each New York Subclass Member will be irreparably harmed unless the Court enjoins Defendant's unlawful, deceptive actions, because, as detailed herein, Defendant will continue to fail to protect Sensitive Information entrusted to it.

104. Plaintiff and New York Subclass Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and

other relief allowable under N.Y. GBL § 349.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(c) For compensatory and punitive damages in amounts to be determined by the Court and/or jury;

(d) For prejudgment interest on all amounts awarded;

(e) For an order of restitution and all other forms of equitable monetary relief;

(f) For an order directing Defendant to cease the illegal actions detailed herein; and

(g) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the Class, demands a trial by jury as to all issues triable of right.

Dated: August 10, 2023

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta
Matthew A. Girardi (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150

Facsimile: (212) 989-9163
Email: pfraietta@bursor.com
mgirardi@bursor.com

BURSOR & FISHER, P.A.
L. Timothy Fisher (*pro hac vice* forthcoming)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

Counsel for Plaintiff